Amendments to the Claims

Please amend Claims 1, 2, 6, 8, 10, 11, 14-17, and 21. The Claim Listing below will replace all prior versions of the claims in the application:

Claim Listing

1. (Currently amended) A system for journaling activity in a data processing system comprising:

a sensor ~~for capturing~~ to sense atomic level events, the sensor located within an operating system kernel within a user client device; and

an aggregator~~, for~~ to accept[[ing]] multiple atomic level events and ~~generating a journal~~ to generate an aggregate event based on a predetermined sequence of atomic level events.

2. (Currently amended) A system as is claim 1 wherein the ~~journal~~ aggregate events are associated with a particular executing process.

3. (Original) A system as is claim 2 wherein the executing process is associated with a particular user.

4. (Original) A system as in claim 1 additionally comprising:

a filter for filtering atomic level events with an approved event list.

5. (Original) A system as is claim 4 wherein the approved event list includes a list of approved file identifiers.

6. (Currently amended) A system as in claim [[4]] 5 wherein the file identifiers are a hash code.

7. (Original) A system as in claim 1, wherein the sensor is located within a client agent and the aggregator is located within a server.

8. (Currently amended) A system as in claim 7 additionally comprising:

a coalescer ~~for coalescing~~ to coalesce multiple atomic events output by the sensor into a single event prior to inputting them to the aggregator.

9. (Original) A system as in claim 8 wherein a bundle of coalesced events is created prior to their transmission between the agent and the server.

10. (Currently amended) A system as in claim [[8]] 9 wherein sequence numbers are added to bundles.

11. (Currently amended) A system as in claim 1 wherein ~~a journal~~ an aggregate event is detected as a suspect action with a data file.

12. (Original) A system as in claim 1 wherein an event is attributable to a known user, thread and/or application as identified at a known time.

13. (Original) A system as in claim 8 wherein the coalescer reports an event after a time out period with no activity.

14. (Currently amended) A system as in claim 1 wherein ~~journal~~ aggregate events are used to control security of the data processing system.

15. (Currently amended) A system as in claim 1 wherein the ~~journal~~ aggregate events are used to provide a perimeter of accountability for file usage at a point of system use.

16. (Currently amended) A system as in claim 15 wherein ~~a~~ the point of use is a user desktop and accountability is of access, modification, and distribution of data files.

17. (Currently amended) A method for journaling activity in a data processing system comprising:

~~capturing~~ sensing atomic level events in an operating system kernel within a user client device; and

aggregating multiple atomic level events to generate ~~a journal~~ an aggregate event based on a predetermined sequence of atomic level events.

18. (Original) A method as in claim 17 additionally comprising:

filtering atomic level events with an approved event list.

19. (Original) A method as in claim 18 where the approved event list includes a list of approved file identifiers.

20. (Original) A method as in claim 17 wherein the step of sensing atomic level events is located within a client agent and the step of aggregating multiple atomic level events occurs within a server.

21. (Currently amended) A method as in claim 20 additionally comprising:

coalescing multiple atomic events output by the sensing step into a single event prior to providing them to the aggregating step.

22. (Original) A method as in claim 21 where a bundle of coalesced events is created prior to a step of transmitting them between the client agent and the server.